PCT/NZ99/00176

09/807482

Intellectual Property Office of New Zealand
Te Pou Rāhui Hanga Hou

REC'D 16 DEC 1999
WIPO PCT

CERTIFICATE

This certificate is issued in support of an application for Patent registration in a country outside New Zealand pursuant to the Patents Act 1953 and the Regulations thereunder.

I hereby certify that annexed is a true copy of the Provisional Specification as filed on 16 October 1998 with an application for Letters Patent number 332374 made by AKTECH LTD.

Dated 7 December 1999.

Neville Harris
Commissioner of Patents

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

332374

Patents Form No. 4 Our Ref: JM502389

Patents Act 1953

PROVISIONAL SPECIFICATION

REMOTE ACCESS AND SECURITY SYSTEM

We, **AKTECH LIMITED**, a New Zealand company, of 20 Malabar Drive, Ellerslie, Auckland, New Zealand, do hereby declare this invention to be described in the following statement:

JM:RM:PT0420596

TECHNICAL FIELD

This invention relates to a remotely operable access and security system.

BACKGROUND

There are many circumstances in which it may be desirable for an owner, operator or manager of items of value to have control over access to that or those items wherever they may be and by whom.

There are many security systems available. In general such security systems may control who has access to the item of value, for example access to buildings or other sites to selected people, such as employees; access to safes, vaults and other such security containers; access to vehicles; access to information and data on a personal computer or a database. These are just a few examples.

In some circumstances existing security systems allow for remote operation of access to a fixed site. In other systems, such as electronically controlled alarms and locks on motor vehicles, the item of value is moveable, but access to it is only controllable at a local level and only by the pre-selected operator.

However, many circumstances exist where security is required in relation to an item or items which do not have a fixed location, and/or for which access is required by a range of different people, perhaps in different circumstances, and for which the owner/operator/manager will wish to retain control over who has access, where and when.

Thus, it is an object of the present invention to provide a method and apparatus for enabling security for and/or access to items of value remotely.

A further or alternative object is to enable security and access control over one or more item of value at any given time or place by any given pre-selected individual, remotely.

Other objects of the present invention may become apparent from the following description which is given by way of example only and with reference to the accompanying drawings.

SUMMARY OF THE INVENTION

According to one aspect of the present invention there is provided a security system adapted to enable controlled access by remote means to one or more value units at any selected place and time and by any selected operator or operators.

According to a further aspect of the present invention there is provided a remote access control system adapted to enable the remote control of access to one or more moveable value units by one or more operators, the system including:

- a central control means including control data relating to the control of access to one or more remote access controller;
- one or more operator control units including actuating means adapted to enable interaction of an operator with the control system;
- one or more access controller, each associated with a value unit and adapted to enable access to the value unit;
- first communication means adapted to provide remote communication between the central control means and one or more operator control units; and
- second communication means adapted to provide remote communication between an operator control unit and one or more access controller.

Preferably, the control system enables a virtual configuration link between the central control means and one or more access controller.

According to a further aspect of the present invention there is provided access control means adapted to enable the remote control of access to one or more value unit, the control means including:

- an access controller associated with the or each value unit, adapted to enable access to the unit and adapted to receive and process control data,
- central control means adapted to generate or enable the generation of control data for controlling the one or more access controllers remote from the central control means,
- one or more operator control units, including actuation means, remote from both the central control means and the one or more access controllers and adapted to enable an operator remote from the central control means to communicate with one or more access controllers to gain access to the or each associated value unit, and
- communication means adapted to enable communication between the central control means and the one or more operator control unit(s), and an operator control unit and one or more access controller(s).

Preferably, the control data may include operator identification code or codes, operator control unit identification code or codes, access controller identification code or codes and access combination or combinations.

Preferably, the or each access controller may include an application template adapted to determine the behaviour of the controller.

Preferably, the control data may further include configuration data for configuring the application template.

Preferably, the configuration data may be encrypted and decipherable only by selected access controllers, creating a virtual configuration link between the central control means and the or each selected access controller.

Preferably, the communication means may include first communication means adapted to enable communication between the central control means and the one or more operator control units, and second communication means adapted to enable communication between an operator control unit and one or more access controllers.

Preferably, the first communication means may include a wide area communication network.

Preferably, the second communication means may include a local area communication link.

According to a further aspect of the invention there is provided a remote access control system substantially as herein described and with reference to the accompanying figures.

Other aspects of the present invention may become apparent from the following description which is given by way of example only and with reference to the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1:

Shows a flowchart representing operation of the system of the present invention.

Figure 2:
Shows a diagrammatic representation of the virtual configuration link involved in the system of the present invention.

Figure 3:
Shows an example of use of the system of the present invention in controlling access to shipping containers

DETAILED DESCRIPTION OF THE INVENTION

In the specification reference is made to centralised management nodes (CMNs) or central control means, personal access nodes (PANs) or operator control units and remote value nodes (RVNs) or access controllers. The term CMN is used to describe an internationally linked database, management and communication system that supplies configuration, access and control information to one or more PAN.

The term PAN is used to describe a personal access device which a pre-authorised person can use to access one or more pre-allocated RVN. Thus, a PAN may be a portable keypad device with communication means enabling it to communicate to the CMN and one or more RVN.

The term RVN is used to describe an electronic control device which is associated with any form of valuable item which requires controllable access. Examples of valuable items (hereafter referred to as "value units") would include shipping containers, retail security cabinets, vending machines, and the like. These examples include locking mechanisms which may be remotely operated. It will be appreciated that there are many other types of value unit which may include locking mechanisms which could be controlled through the system of the present invention, such as personnel security access. In addition, the invention may be equally applicable to the control of access to different types of value unit, such as data and information, via

security systems other than physical locks. This may include, for example, internet access, smart card cash transfer, and access to electronic databases of any type .

A PAN provides a configuration, access and control link between the CMN and one or more RVN. Communication between the CMN and the or each PAN is via, for example, direct serial link using local PC connections, one or two-way pager networks, a two-way cellphone network or other means of wide area data communication.

Communication between a PAN and one or more RVN is via local area communication means, such as an infrared link, a local area RF link, acoustic coupling or a direct connect link.

A RVN may include a controller unit and an associated locking mechanism. For security reasons a RVN may be located within its associated value unit. For example, if the item is a shipping container or vending machine, then the RVN would be inside that container or machine, would preferably be communicated to by the PAN by remote means, and would therefore be inaccessible except via access to the value unit by an operator of the PAN.

Any given RVN controller has an application template. The nature of this template will depend on the nature of the value unit controlled by the RVN. It would include, as a minimum, an access combination. It may also include: time and location criteria, if the item is one which may only be accessed at specific times or dates, or at specific locations (for example controlled by a GPS unit); control criteria, such as how often the unit may be accessed, how long the unit is accessible after access is provided, etc; user/operator group access criteria; and encryption criteria.

An RVN controller may have a plurality of application templates so that it may be adapted to operate in a number of different ways.

The application template is specific to each RVN application. Using the template a RVN can be configured to suit a variety of applications, different applications being appropriate for different value units and in different circumstances.

The system of the present invention enables the controlled access to a RVN (or many of them) from the CMN by employing a virtual configuration link between the CMN and the RVN, via the PAN.

Operation of the system of the present invention is now described in broad terms with reference to Figure 1.

Each PAN has a unique identification number. A PAN is "activated" by communication of its correct identification number from the CMN (steps 1 and 2 of Figure 1). Any given user or operator of a PAN has an access or PIN number. The CMN loads one or more user authorisation to the PAN (step 3) in the form of the access or PIN number.

The CMN then also loads to the PAN one or more identification numbers for one or more RVN which is to be accessed by the PAN (step 4). Hence, a single PAN may be authorised to enable access to multiple RVNs.

An application template for the or each RVN is then downloaded from the CMN to the PAN (step 5). This application template may be in an encrypted form such that it can only be deciphered by the RVN. This creates a "virtual configuration link" between the CMN and the remote RVN. The application template will only usually be downloaded to the RVN during the commissioning stage, when the RVN is initialised with the required template.

The CMN also downloads to the PAN device configuration data for the selected RVN (step 6). Again this may be in an encrypted form, only able to be deciphered by the relevant RVN.

Once all necessary data has been communicated from the CMN to the PAN, and a selected operator has correctly identified themselves to the PAN using their access or PIN number, the PAN communicates via a local area communications link to the or each RVN (steps 7 and 8). The PAN will download the application template to a correctly identified RVN (step 9). The PAN then downloads configuration, access and control data to the RVN (steps 10 and 11). The controller of the RVN deciphers this data, if encrypted, and uses the data to validate remote access to the RVN (steps 12 and 13).

It will be appreciated that each PAN may have one or more assigned operators and can be programmed to access one or more RVN.

Configuration data is used to initialise the behaviour of a RVN. The data will be directly related to the configuration structure of the application template.

Access and control data is "known" to the PAN and may, for example, contain user identification/PIN numbers, the PAN identification number and access combination details.

The virtual configuration link involved in the system of the present invention is summarised in Figure 2. Normally there is no direct communication link between the CMN and a RVN. A PAN provides a virtual configuration link between the CMN and a RVN by creating a virtual security tunnel. The CMN sends encrypted RVN-specific configuration information to the PAN. The PAN does not have access to the encrypted configuration information because it does not have the required deciphering codes. When the PAN communicates with a remote RVN the configuration information is

downloaded to the RVN which then deciphers the information and updates the RVN configuration. The RVN can then process the user level access and control data, also communicated from the PAN.

An example of the system of the present invention in operation is now presented with specific reference to the control of access to a shipping container. It will be appreciated that shipping containers are a good example of a value unit which does not have a fixed location and which may need to be accessed at different times, in different places by a variety of different operators.

A RVN controller may be located inside a shipping container for controlling the locking mechanism. There would be no physical connection between the RVN and the outside of the container, except for a communication pod enabling communication between the controller and a PAN. Reference is now made to Figure 3. A remote shipping agent 1 requiring access to a container 2 at the port of destination would communicate their need to access the container to the local shipping agent or security manager 3. Alternatively, this communication may be unnecessary if the RVN in that container has been pre-programmed to enable access at specific locations and times.

The local shipping agent or security manager authorises the remote agent to access a designated container by sending authorisation data to the PAN 4 via the CMN 5. This communication is shown as being via a locally linked PC connection 6 and a wide area communications network 7.

The remote agent 1 uses an activated PAN to transfer configuration, access and control information to the relevant RVN and thus obtain access to the container 2.

Thus, using a system of the present invention an owner/manager of value units which have no fixed location can provide security access to that or those items at any given time or place and only by authorised users/operators. The unit itself has no fixed

external keypad or means of direct communication with the PAN. Furthermore, control intelligence relating to a particular RVN is held in the CMN and not in the RVN itself. Additional security is provided by encryption of data to provide a virtual communication link between the CMN and RVN. The encryption method may include code hopping algorithms communicated between the CMN and RVN via the PAN for added security.

Where in the foregoing description reference has been made to specific components or integers of the invention having known equivalents then such equivalents are herein incorporated as if individually set forth.

Although this invention has been described by way of example and with reference to possible embodiments thereof it is to be understood that modifications or improvements may be made thereto without departing from the scope or spirit of the invention.

AKTECH LIMITED

By its Attorneys
BALDWIN SHELSTON WATERS

JM:RM:LAVA:SPEC:
File Ref: 502389

332374

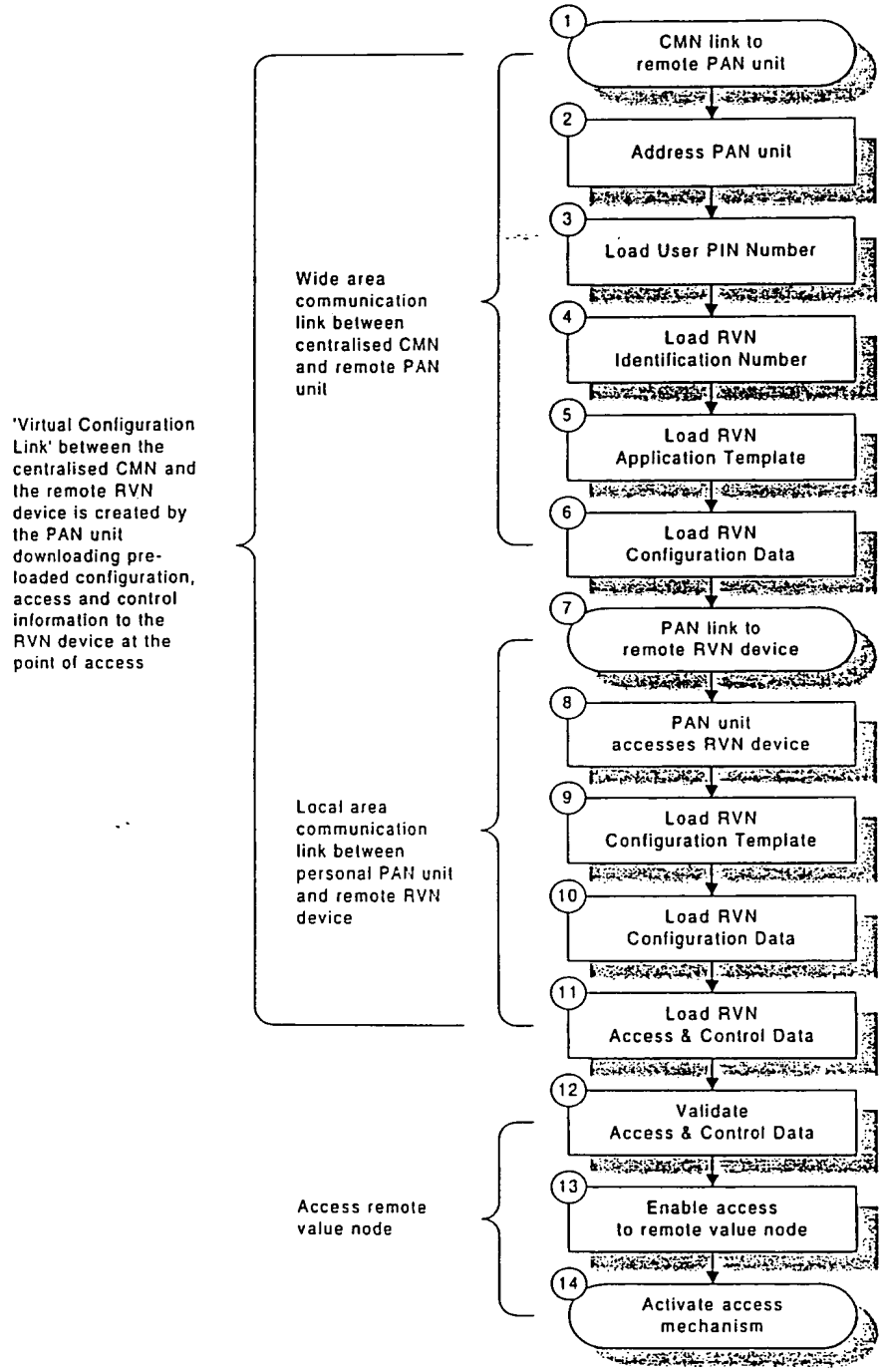

'Virtual Configuration Link' between the centralised CMN and the remote RVN device is created by the PAN unit downloading pre-loaded configuration, access and control information to the RVN device at the point of access
Wide area communication link between centralised CMN and remote PAN unit
Local area communication link between personal PAN unit and remote RVN device
Access remote value node
1 CMN link to remote PAN unit
2 Address PAN unit
3 Load User PIN Number
4 Load RVN Identification Number
5 Load RVN Application Template
6 Load RVN Configuration Data
7 PAN link to remote RVN device
8 PAN unit accesses RVN device
9 Load RVN Configuration Template
10 Load RVN Configuration Data
11 Load RVN Access & Control Data
12 Validate Access & Control Data
13 Enable access to remote value node
14 Activate access mechanism

FIGURE 1

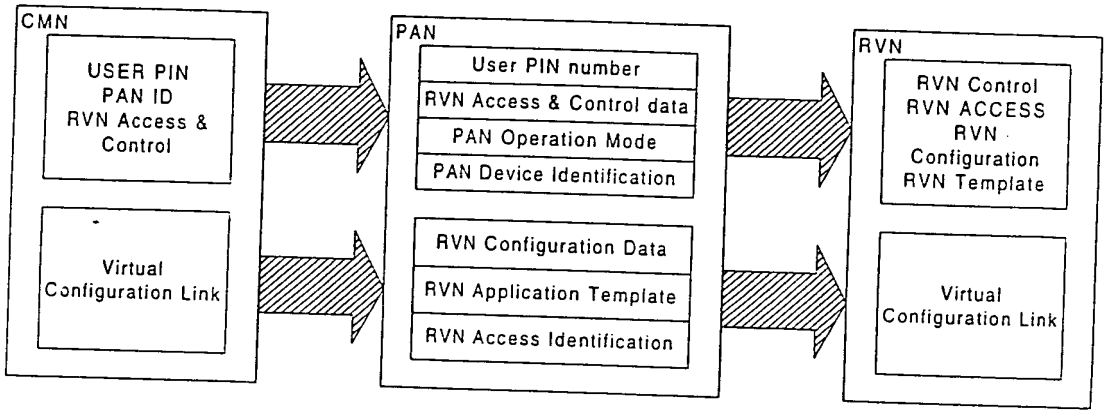
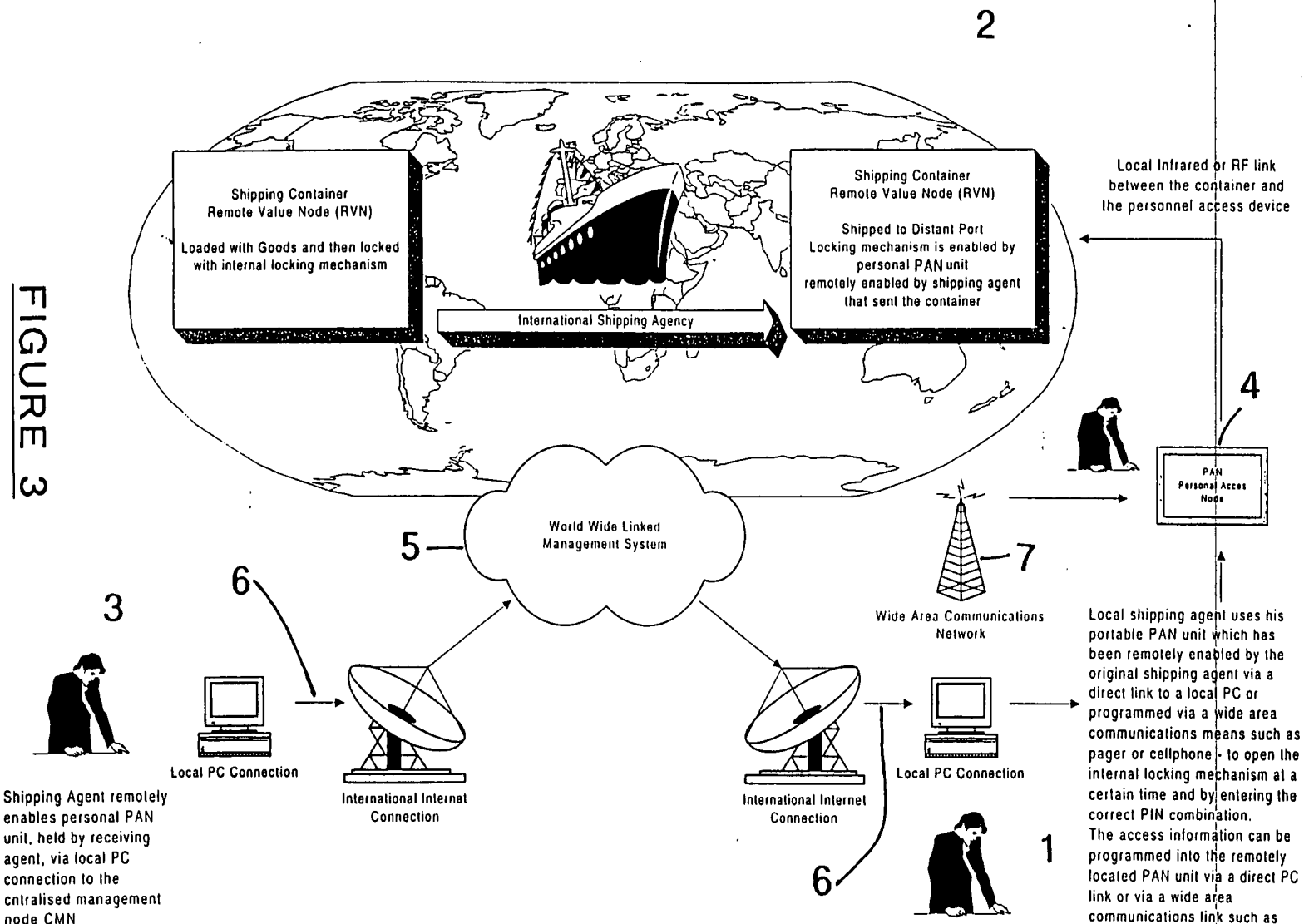

CMN
USER PIN
PAN ID
RVN Access &
Control
Virtual
Configuration Link
PAN
User PIN number
RVN Access & Control data
PAN Operation Mode
PAN Device Identification
RVN Configuration Data
RVN Application Template
RVN Access Identification
RVN
RVN Control
RVN ACCESS
RVN
Configuration
RVN Template
Virtual
Configuration Link

FIGURE 2

FIGURE 3


2
Shipping Container
Remote Value Node (RVN)
Loaded with Goods and then locked
with internal locking mechanism
International Shipping Agency
Shipping Container
Remote Value Node (RVN)
Shipped to Distant Port
Locking mechanism is enabled by
personal PAN unit
remotely enabled by shipping agent
that sent the container
Local Infrared or RF link
between the container and
the personnel access device
4
PAN
Personal Acces
Node
5
World Wide Linked
Management System
7
Wide Area Communications
Network
6
3
Local PC Connection
International Internet
Connection
International Internet
Connection
Local PC Connection
6
1
Shipping Agent remotely
enables personal PAN
unit, held by receiving
agent, via local PC
connection to the
cntralised management
node CMN
Local shipping agent uses his
portable PAN unit which has
been remotely enabled by the
original shipping agent via a
direct link to a local PC or
programmed via a wide area
communications means such as
pager or cellphone - to open the
internal locking mechanism at a
certain time and by entering the
correct PIN combination.
The access information can be
programmed into the remotely
located PAN unit via a direct PC
link or via a wide area
communications link such as
pager or cellphone networks